# EFFICIENT STREAM CIPHER SYSTEM AND METHOD

## ABSTRACT OF THE INVENTION

A computer system and method generates a random output stream of bits. The system comprises an initial evolving state produced from one or more initial keys, one or more round functions, and one or more mask tables. Each round function is part of a step in a sequence of steps. Each step applies the respective round function to a current evolving state to produce a respective new evolving state for processing by the next step in the sequence. The first step in the sequence starts b processing the initial evolving state. The mask tables are produced from one or more of the initial keys. Each of the mask tables has one or more masks. The masks are combined, in each respective step, with the respective new evolving state in a combination operation to create a respective step output. The random output stream bits is a concatenation of each of the respective step outputs. In one preferred embodiment, one or more of the masks in the mask tables are replaced by one or more replacement masks after a number of combination operations. The replacement masks not being linear combinations of prior masks. In an alternative embodiment, there are two or more mask tables produced from one or more of the initial keys. One or more of the masks from each table is combined, in each respective step, with the respective new evolving state in a combination operation to create a respective step output. There may or may not be replacement of the masks in this embodiment.